Listing of Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (withdrawn) A method of mirroring security processors comprising the steps of:

generating information for a first security processor;

repeatedly sending the information to a second security processor in accordance with the first security processor processing at least one packet.

2. (withdrawn) The method of claim 1 wherein the sending step comprises sending the information from the first security processor to the second processor.

3. (withdrawn) The method of claim 1 wherein the generating step comprises generating the information in the first security processor.

4. (withdrawn) The method of claim 1 further comprising the step of generating at least one packet including the information, wherein the sending step comprises sending the at least one packet over a packet network.

5. (withdrawn) The method of claim 1 wherein the sending step further comprises sending the information over a dedicated link between the first security processor and the second security processor.

6. (withdrawn) The method of claim 5 wherein the dedicated link comprises an Ethernet link.

7. (withdrawn) The method of claim 1 wherein the sending step comprises repeatedly sending the information on a per-packet basis.

8. (withdrawn) The method of claim 1 wherein the sending step comprises repeatedly sending the information at intervals according to at least one sequence number.

9. (withdrawn) A method of mirroring security processors comprising the steps of:

generating security association information for a first security processor; and

repeatedly sending the security association information to a second security processor in accordance with the first security processor processing at least one packet.

10. (withdrawn) The method of claim 9 wherein the information comprises at least one security association sequence number.

11. (withdrawn) The method of claim 9 wherein the information comprises at least one security association byte count.

12. (withdrawn) The method of claim 9 wherein the sending step further comprises repeatedly sending the security association information on a per-packet basis.

13. (withdrawn) The method of claim 9 wherein the sending step further comprises repeatedly sending the security association information at intervals according to at least one sequence number.

14. (withdrawn) The method of claim 9 further comprising the step of generating at least one packet including the security association information, wherein the sending step comprises sending the at least one packet.

15. (withdrawn) The method of claim 9 further comprising the step of generating at least one packet including the security association information, wherein the sending step comprises sending the at least one packet over a packet network.

16. (withdrawn) The method of claim 9 wherein the sending step further comprises sending the information over a dedicated link between the first security processor and the second security processor.

17. (withdrawn) The method of claim 16 wherein the dedicated link comprises an Ethernet link.

18. (previously presented) A method of providing redundancy in a security processing system comprising the steps of:

establishing a first secure packet flow through a first security processor;

updating a parameter in a set of parameters of a security association associated with the first secure packet flow;

establishing a second secure packet flow through a second security processor;

updating a parameter in a set of parameters of a security association associated with the second secure packet flow;

sending the updated parameter associated with the first secure packet flow from the first security processor to the second security processor in a first update packet when a sequence number in the set of security association parameters associated with the first secure packet flow reaches a first predefined value;

sending the updated parameter associated with the second secure packet flow from the second security processor to the first security processor in a second update packet when a sequence number in the set of security association parameters associated with the second secure packet flow reaches a second predefined value; and

storing the updated parameter associated with the first secure packet flow and the updated parameter associated with the second secure packet flow in the first security processor and in the second security processor.

19. (previously presented) The method of claim 45 wherein the rerouting step is in response to a failure of packet flow through the first security processor.

20. (canceled)

21. (previously presented) The method of claim 18 wherein the sequence number in the set of security association parameters associated with the first secure packet flow is incremented when a packet in the first secure packet flow is received from or transmitted to a network.

22. (previously presented) The method of claim 18 wherein the updated parameter associated with the first secure packet flow comprises a at least one byte count.

23-24. (canceled)

25. (previously presented) The method of claim 18 further comprising the step of generating at least one configuration packet including the updated parameter associated with the first secure packet flow, wherein sending the updated parameter from the first security processor to the second security processor comprises sending the at least one configuration packet.

26. (previously presented) The method of claim 18 further comprising the step of sending, by a host processor, configuration information to the first security processor and the second security processor.

27. (previously presented) The method of claim 18 further comprising the step of sending, by a host processor, security association configuration information to the first security processor and the second security processor.

28. (canceled)

29. (previously presented) The method of claim 18 further comprising the steps of:

defining a quantity to adjust the sequence number in the set of parameters of the security association associated with the first secure packet flow;

defining an interval at which to update the set of parameters of the security association associated with the first secure packet flow; and

determining whether to send the updated parameter associated with the first secure packet flow to the second security processor according to a comparison of the sequence number with the interval.

30. (previously presented) The method of claim 29 further comprising adding the quantity to the sequence number before sending the updated parameter associated with the first secure packet flow to the second security processor.

31-33. (canceled)

34. (previously presented) The method of claim 18 further comprising the step of sending replay window information to the second security processor.

35. (withdrawn) A security processing system, comprising:

a first security processor for processing packets and for updating security association information associated with the packets, the first security processor comprising at least one MAC for sending updated security association information over a packet network; and

a second security processor for receiving the updated security association information over the packet network.

36. (withdrawn) The security processing system of claim 35 further comprising at least one host processor connected to the first security processor and the second security processor for terminating or initiating the packets.

37. (withdrawn) The security processing system of claim 36 wherein the at least one host processor changes the routing of packet flow by either routing the packets to the second security processor instead of the first security processor.

38. (previously presented) A security processing system, comprising:

a first security processor configured to process a first packet flow, update a parameter in a set of parameters of a security association in response to the first packet flow, and send the updated parameter associated with the first packet flow in a first update packet when a sequence number in the set of security association parameters associated with the first packet flow reaches a first predefined value; and

a second security processor configured to process a second packet flow, update a parameter in a set of parameters of a security association in response to the second packet flow, and send the updated parameter associated with the second packet flow in a second update packet when a sequence number in the set of security association parameters associated with the second packet flow reaches a second predefined value,

wherein the first security processor is further configured to send the updated parameter in response to the first packet flow to the second security processor at a first predefined interval and the second security processor is further configured to send the updated parameter in response to the second packet flow to the first security processor.

39. (previously presented) The security processing system of claim 46 wherein the at least one host processor is connected to at least one switch for terminating or initiating the first packet flow and the second packet flow.

40. (previously presented) The security processing system of claim 39 wherein the at least one host processor changes the routing of packet flow by either routing the first packet flow to the second security processor instead of the first security processor or

routing the second packet flow to the first security processor instead of the second security processor.

41. (previously presented) The security processing system of claim 40 wherein the change in the routing is in response to a failure of the first packet flow through the first security processor or the second packet flow through the second security processor.

42. (canceled)

43. (previously presented) The security processing system of claim 46 wherein the at least one host processor routes the first packet flow to the second security processor instead of the first security processor.

44. (previously presented) The security processing system of claim 43 wherein the at least one host processor routes the second packet flow to the first security processor instead of the second security processor.

45. (previously presented) The method of claim 18, further comprising:

rerouting the first secure packet flow to flow through the second security processor instead of the first security processor

46. (previously presented) The security processing system of claim 38, further comprising:

at least one host processor for establishing first packet flow to the first security processor and the second packet flow to the second security processor.